Голові разової спеціалізованої вченої ради Національного університету «Київський авіаційний інститут»

д.т.н., проф. Одарченку Роману Сергійовичу
пр. Любомира Гузара 1, м. Київ, 03058, Україна

РЕЦЕНЗІЯ
Ахрамовича Володимира Миколайовича
доктора технічних наук, професора,
професора кафедри кібербезпеки
Факультету комп'ютерних наук та технологій Національного
університету «Київський авіаційний інститут»
на дисертаційну роботу Юдіної Діани Олексіївни
на тему «Методи та моделі оцінювання стану кіберзахисту об'єктів критичної інформаційної інфраструктури»,
представлену на здобуття наукового ступеня доктора філософії
за спеціальністю 122 – Комп'ютерні науки
галузі знань 12 – Інформаційні технології

1. Актуальність теми дисертаційного дослідження.

Сучасні об'єкти критичної інформаційної інфраструктури (ОКІІ) характеризуються високим рівнем гетерогенності програмно-апаратних платформ, де застарілі промислові контролери й операційні технології (ОТ) співіснують із сучасними хмарними сервісами та розподіленими ІТ-мережами. Така складність архітектури створює серйозні інженерно-програмні виклики при побудові автоматизованих систем підтримки прийняття рішень у галузі комп'ютерних наук.

Основна науково-прикладна проблема полягає в тому, що існуючий аналітичний та програмний інструментарій спирається на статичні алгоритми оцінювання, які не спроможні адаптуватися до унікальної конфігурації конкретного об'єкта. При намаганні звести різнорідні технологічні параметри до єдиного показника виникають значні обчислювальні викривлення, а також втрачається інформація про критичні вразливості на стиках між ІТ- та ОТ-сегментами.

З точки зору комп'ютерних наук, виникає гостра потреба у створенні модульного обчислювального апарату, здатного динамічно формувати оціночні профілі під будь-яку з 24 галузей критичної інфраструктури, опрацьовувати великі масиви даних та виконувати інтелектуальну фазифікацію оцінок у межових зонах невизначеності.

У зв'язку з цим, розроблення гібридних математичних моделей, багатокритеріальних алгоритмів із залученням нечіткої логіки та їхня практична реалізація у вигляді кросплатформного програмного комплексу для оцінювання стану кіберзахисту ОКІІ є актуальним, обчислювально обґрунтованим і практично значущим науково-прикладним завданням спеціальності 122 «Комп'ютерні науки».

2. Зв'язок роботи з науковими програмами, планами, темами

Тема дисертації узгоджена з освітньо-науковою програмою за спеціальністю 122 «Комп'ютерні науки» та є складовою частиною виконання НДР Державного університету «Київський авіаційний інститут» «Методи, моделі та програмні засоби управління інцидентами кібербезпеки в критичній інфраструктурі держави» (державний реєстраційний номер 0125U000624).

3. Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих у дисертації

Обґрунтованість наукових результатів забезпечена коректною систематизацією вхідних даних, застосуванням апарату теорії множин, теорії нечітких множин, багатокритеріального аналізу (MAI) та теорії прийняття рішень.

Достовірність підтверджена результатами експериментального дослідження на об'єкті паливно-енергетичного сектору, програмною реалізацією та актами впровадження у практичну діяльність державних органів і науково-дослідний процес.

4. Наукова новизна результатів дослідження

Наукова новизна одержаних результатів полягає у розв'язанні актуального наукового завдання з розробки методів та моделей оцінювання стану кіберзахисту ОКІІ:

Вперше:

- розроблено гібридну ієрархічну модель системи показників кіберзахисту ОКІІ, яка, на відміну від існуючих, базується на ієрархічній декомпозиції семи функціональних систем критеріїв (шість з яких гармонізовано з міжнародним фреймворком NIST CSF 2.0, а сьома – «Секторальна складова»), що дозволило вперше в межах єдиного оціночного циклу врахувати специфічні вимоги 24 галузей критичної інфраструктури України;
- обґрунтовано метод багатокритеріального оцінювання стану кіберзахисту, який відрізняється від відомих інтеграцією процедури перевірки нормативної відповідності з механізмом попарних порівнянь для пріоритезації захисних заходів, що забезпечило можливість формалізувати неоднаковий вплив різних систем захисту на інтегральний рівень безпеки об'єкта.

Удосконалено:

- математичну модель нечіткої інтерпретації стану кіберзахисту, яка, на відміну від традиційних підходів, використовує нечіткі числа LR-типу трапецієподібної форми та розрахунок індексу впевненості, що дало змогу підвищити точність оцінювання у межових зонах між рівнями захищеності;
- процедуру формування якісних висновків щодо стану кіберзахисту шляхом впровадження апарату асоціативних правил до результатів фазифікації інтегрального показника, що дозволило констатувати поточний рівень захищеності та здійснювати прогнозування стійкості системи до дестабілізуючих впливів.

Отримала подальший розвиток:

класифікація рівнів зрілості процесів кіберзахисту, яка відрізняється врахуванням факторів воєнного стану та динамічної природи атак, що

дозволило диференціювати стан захищеності об'єктів за уточненою п'ятирівневою шкалою.

5. Повнота викладу матеріалів дисертації в опублікованих працях, персональний внесок здобувача

Основні наукові результати дисертаційного дослідження відображено у 8 наукових публікаціях. Серед них: 7 фахових статей у виданнях України зі спеціальності 122 (3 статті одноосібні) та 1 публікація у матеріалах міжнародної конференції IEEE ATIT 2024, що індексується у Scopus. Особистий внесок здобувачки у роботах, виконаних у співавторстві, полягає у проведенні аналітичних досліджень, розробці математичних моделей, програмного коду та проведенні обчислювальних експериментів.

6. Практичне значення отриманих результатів

Практична цінність результатів дисертації полягає у створенні автоматизованого інструментарію оцінювання стану кіберзахисту.

Зокрема:

- реалізовано програмний продукт «Програмний компонент оцінювання рівня кіберзахисту ОКІІ» (Свідоцтво про реєстрацію авторського права № 145206);
- сформовано систему з 106 базових та 91 галузевого критерію;
- теоретичні та практичні результати впроваджено в Адміністрації Державної служби спеціального зв'язку та захисту інформації України, Державному науково-дослідному інституті технологій кібербезпеки та захисту інформації, а також у НДЛ протидії кіберзагрозам в авіаційній галузі Державного університету «Київський авіаційний інститут».

7. Структура та зміст дисертації

Дисертація є цілісною, завершеною науковою працею. Вона містить вступ, 4 розділи, висновки, список використаних джерел та додатки з лістингом коду і актами впровадження.

Зміст розділів:

У першому розділі проведено аналіз сутнісних характеристик оцінювання кіберзахисту. Виконано систематизацію трьох основних методологічних напрямів: на основі зрілості (CMMI, C2M2), на основі відповідності (ISO/IEC 27001, NIST SP 800-53A, PCI DSS) та на основі ризиків (FAIR, CISA CPGs). Побудовано порівняльну характеристику структурних компонентів міжнародних стандартів (ISO/IEC 27001:2022, NIST CSF 2.0, ENISA EUCS). Обґрунтовано обмеження щодо копіювання міжнародних стандартів в умовах воєнного стану. Проведено аналіз методів агрегування показників та висвітлено переваги методу аналізу ієрархій (MAI) для розв'язання задачі зважування критеріїв.

У другому розділі розроблено концептуальну структуру гібридної ієрархічної моделі. Здійснено теоретико-множинну формалізацію множин критеріїв, що охоплює 6 функціональних систем NIST CSF 2.0 («Govern», «Identify», «Protect», «Detect», «Respond», «Recover») та 7-му систему – «Секторальну складову». Загалом формалізовано 106 базових та 91 галузевий критерій. Розроблено математичну модель нечіткої інтерпретації результатів із формулюванням лінгвістичної змінної CSL («Стан кіберзахисту») та побудовою трапецієподібних функцій належності LR-типу для 5 еталонних станів.

У третьому розділі обґрунтовано дискретну шкалу квантифікації. Описано розрахунок вагових коефіцієнтів за допомогою попарних порівнянь MAI. Викладено каскадну схему обробки даних з обчисленням нормалізованого індексу впевненості (ECI) та базу нечітких асоціативних правил.

У четвертому розділі наведено опис програмної архітектури кросплатформного застосунку. Викладено результати експериментальної валідації методу на об'єкті паливно-енергетичного сектору (7 експертів) та наведено порівняльний аналіз ефективності.

8. Оцінка мови та стилю дисертації. Дискусійні зауваження. Дані про відсутність текстових запозичень та порушень академічної доброчесності

Дисертація викладена з дотриманням вимог академічного стилю та наукової мови.

Висловлю такі дискусійні зауваження:

1. У другому розділі при специфікації системи «Секторальна складова» для різних секторів критичної інфраструктури міститься від 3 до 5 критеріїв. Варто було б детальніше висвітлити вплив такої нерівномірності кількості показників на загальну вагову значимість системи.

2. У третьому розділі при каскадній обробці даних використовується нормалізований індекс впевненості. Бажано розширити аналіз граничного випадку, коли індекс впевненості отримує однакові значення для двох сусідніх станів (наприклад, 0,5 та 0,5).

3. У четвертому розділі програмний компонент реалізовано як настільний застосунок. У роботі було б доцільно вказати вимоги до обчислювальних ресурсів при масовому опитуванні великої кількості ОКІІ.

4. В основному тексті трапляються поодинокі друкарські помилки у позначеннях окремих індексів у математичних формулах розділу 3 та деякі неточності формулювання – розділ 2.

Академічна доброчесність: Порушень принципів академічної доброчесності, плагіату чи фальсифікацій даних не виявлено. Дисертація є оригінальною працею.

9. Відповідність фаху

Дисертаційна робота Юдіної Д.О. за своєю тематикою, методологічним апаратом та практичними результатами повністю відповідає паспорту спеціальності 122 – Комп'ютерні науки (галузь знань 12 – Інформаційні технології).

10. Відповідність дисертації встановленим вимогам

Дисертація Юдіної Діани Олексіївни є завершеною кваліфікаційною працею, у якій отримано нові обґрунтовані результати, що розв'язують актуальне науково-прикладне завдання комп'ютерних наук.

Дисертація «Методи та моделі оцінювання стану кіберзахисту об'єктів критичної інформаційної інфраструктури» відповідає вимогам «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженого постановою Кабінету Міністрів України від 12 січня 2022 р. № 44 (зі змінами).

Її авторка, Юдіна Діана Олексіївна, заслуговує на присудження наукового ступеня доктора філософії за спеціальністю 122 – Комп'ютерні науки.

Рецензент:
професор кафедри кібербезпеки
Факультету комп'ютерних наук та технологій КАІ
доктор технічних наук, професор Володимир АХРАМОВИЧ

Підпис Ахрамовича В.
особистий підпис
ЗАСВІДЧУЮ
ВЧЕНИЙ СЕКРЕТАР
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»
Ірина Набоа